REMARKS

Given the lengthy prosecution history of this application, Applicants wish to immediately note the following feature in the Angelo reference (USP 5,923,754). Consider Figure 3 which shows that the Angelo DVD disk stores a "disk key" (element 56). This disk key is retrieved by the DVD drive, encrypted and sent to the video controller. As shown in step 66, the video controller decrypts the disk key. Then in step 72, the video controller decrypts the content on the disk using the disk key.

But note the flaw that could be exploited by a hacker – suppose the hacker does not use an "Angelo" DVD disk drive but instead retrieves the disk key from the DVD disk using an DVD reader. This disk key may then be readily used to decrypt the content on the disk. In sharp contrast, claim 1 recites the generation (within the storage engine) of a combination key "by combining a medium key with the internal key [generated by the storage engine]." Then, within the storage engine, the content is decrypted with the combination key. Thus, the key to decrypting the content (the combination key) is not stored on the medium. Instead, the combination key is generated within the storage engine (thus being safe from hackers) wherein this combination key is what decrypts the content.

Applicants respectfully submit that that indeed claim 1 would be anticipated were applicants to claim the following scheme: retrieve a disk key from the media, encrypt it into a combination key and send the combination key to a video controller, decrypt the combination key in the video controller to retrieve the disk key, and then decrypt content with the disk key. That is the scheme disclosed by Angelo and as noted above, is inherently vulnerable to hacking.

In sharp contrast, claim 1 recites the act of "within the data storage engine, decrypting a first portion of data stored on the storage medium with said first combination key." Advantageously, the combination key never leaves data storage engine (whereas it does in

PAGE 10/12 * RCVD AT 6/8/2005 6:45:38 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:9497527049 * DURATION (mm-ss):03-20

Angelo, thereby exposing the transfer to hackers). Moreover, it is the combination key that is used within the data storage engine to decrypt the content. Unlike the disk key in Angelo, this combination key is never stored on the storage medium and is thus immune to hackers. Accordingly, because the advantageous method recited in claim 1 is neither suggested nor taught by Angelo, Applicants respectfully submit that claim 1 is patentable over this reference.

Claims 22 through 25 stand withdrawn as being directed to a non-elected species.

PAGE 11/12 * RCVD AT 6/8/2005 6:45:38 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:9497527049 * DURATION (mm-ss):03-20

CONCLUSION

For the above reasons, pending Claims 1 – 3, and 6 – 21 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

I hereby certify that this correspondence is facsimile transmitted to the Commissioner for Patents, Washington, D.C. 20231, at 703-872-9306, on June 8, 2005.

Saundra L. Carr

June 8, 2005
Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,622

PAGE 12/12 * RCVD AT 6/8/2005 6:45:38 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:9497527049 * DURATION (mm-ss):03-20